Accessing Aeronautical Information from NGA

https://www.extranet.nga.mil

December 01, 2005

The National Geospatial-Intelligence Agency (NGA) will remove DAFIF™ and FLIP data from the NGA public web site on October 1, 2006. Department of Defense (DoD) customers will be able to access DAFIF™ and FLIP information after October 1, 2006 by accessing the NGA's web site on the NIPRNet. The NGA NIPRNet site, in accordance with a number of DoD directives, will be Public Key Enabled (PKE); meaning that the site will be encrypted using the DoD Public Key Infrastructure (PKI).

DoD PKI on the NIPRNet will provide the required security that will allow NGA to continue to make DAFIF™ and FLIP data available.

Reasons for choosing the PKE-NIPRNet network to host FLIP and DAFIF™ data:

- Many countries have copyrighted the information NGA makes available as DAFIF™ and FLIP data. In the past NGA has released that information to the public at no charge effectively nullifying the copyright. To continue to receive that foreign information NGA must restrict access to only DoD customers.
- There is currently NO other alternative infrastructure at NGA to host this data which provides the required protection for the data. A "reverse domain lookup" to restrict access to .mil and .gov networks does not provide sufficient safeguards for the data.
- PKI offers higher identity-assurance and removes the need for passwords. Reference DoD's PKE Instruction 8520.
- Using the NIPRNet coincides with a pre-existing plan to host all unclassified NGA data on that network.
- Users now receiving DAFIF™ and FLIP data on CDs/DVDs from the Defense Logistics Agency (DLA) will not experience any changes.

Other Services/Agencies may choose to re-host DAFIF™ and FLIP data on their own protected sites. However, after existing sites are public-key enabled (e.g. no more usernames and passwords), it is suggested that links be provided to avoid the cost of re-hosting the same data. In addition the Service/Agency that does choose to re-host must ensure that:

- The data is not available to the public, and
- the data is kept current

NGA's, foreign, data co-producers currently download/utilize DAFIF™ and FLIP data from the NGA public web site. These entities will not be allowed access to the data after October 1, 2006 until they have established a Memorandum of Agreement (MOA) with NGA's Office of International and Policy (OIP). The MOA will indicate the new method of obtaining the DAFIF™ and FLIP data after October 1, 2006.

NGA's PKE NIPRNet CHARTER

The NGA PKE-NIPRNet is intended to be a protected portal to NGA products for the DoD, Intelligence Community (IC), and other government agencies. Goals of the NGA PKE-NIPRNet infrastructure include:

- **High Availability** - NGA's PKE NIPRNet shall include no less than two fully-redundant, replicated, geographically-separated, load-balanced systems with automatic failover
- **Internet Accessibility** - NGA's PKE NIPRNet shall be accessible from the Internet for users with DoD's PKI certificates which do not have access to dedicated NIPRNet terminals.
- **Expandability & Scalability** - NGA's PKE NIPRNet infrastructure shall accommodate the addition of any number of servers
- **Information Assurance** – Information assurance shall be achieved by the use of communication-encryption technologies, such as SSL, and the use of digital identification-certificates
    - DoD's Public-Key-Enabling Instruction 8520.2 directs:
        - Private web servers should be PK-enabled to use server certificates for confidentiality. This involves obtaining and installing a web-server certificate and enabling the Secure Sockets Layer (SSL) protocol on every web server . Consequently, all communication is encrypted between a web server and the web browser .
        - Private web servers should also be PK-enabled to require client-based-certificate authentication. This requires the web server to have a certificate and each authorized user of the web server to have an identity certificate.

The need to utilize web-based technologies to provide a secure and consistent access for NGA's resources drove the creation of NGA's PKE NIPRNet. Today, the infrastructure:

- Encrypts web-data transactions using the Secure Sockets Layer (SSL) protocol.
- Provides PK-enablement for any future PKE-NIPRNet application and web-servers
- Centralizes PKI authentication/authorization for holders of DoD's PKI certificates
- Provides single-sign-on capabilities
- Provides Communities of Interest (COI) workgroups –
    - Private COI's: secured, exclusive, private web space to authorized PKE-NIPRNet users for sharing/collaboration of private/secured information.
    - Public COI's: open to all PKE-NIPRNet users for viewing public information.
- Provides a fully-redundant capability for failover and load balancing
- Provides an expandable infrastructure

Why use PKI?

The Deputy Secretary of Defense issued the following memorandum for all defense systems on 10 November 1999:

"The initial implementation of smart card technology shall be effected as a Department-wide common access card (CAC). The CAC shall be the standard ID card for active duty military personnel (to include the Selected Reserve), DoD civilian employees and eligible contractor personnel. It also will be the principal card used to enable physical access to buildings and controlled and will be used to gain access to the Department's computer networks and systems..."

"...In response to the increasing threat to our networks and computer systems, I previously mandated DoD-wide movement toward a ubiquitous public key infrastructure (PKI)." (Hamre J, Deputy Secretary of Defense)

Additional DoD policies that shaped NGA's PKE NIPRNet are:

- Memorandum - Public Key Enabling (PKE) of Applications, Web Servers, and Networks for the Department of Defense, dated 17 May 2001DoD Mandate DoD PKI PK Enabling Instruction 8520.2. NSTISSP 11 - Information Assurance (IA) shall be considered as a requirement for all systems used to enter, process, store, display, or transmit national security information. IA shall be achieved through the acquisition and appropriate implementation of evaluated or validated Government Off-the-Shelf (GOTS) or Commercial Off-the-Shelf (COTS) IA and IA-enabled Information Technology (IT) products. These products should provide for the *availability* of the systems; ensure the *integrity* and *confidentiality* of information, and the *authentication* and *non-repudiation* of parties in electronic transaction

Getting Started

- Obtain a DoD-PKI certificate (see section below)
    - Common Access Card (CAC)
    - Software Certificate
- Register with the system – https://www.extranet.nga.mil
    - Provide basic, personal information
    - Provide a Security Personnel POC that can authoritatively confirm a user's citizenship and clearance information.
        - There is an ongoing search for web services that can authoritatively confirm a user's citizenship and clearance
    - Provide Supervisor/Contracting Officer Technical Representative (COTR) POC to verify user's Need-to-Know
    - Provide Supervisor/COTR (for CONTRACTORS only) to verify contract number, contract start date and contract end date

Obtaining a DoD-PKI Certificate

- CACs come with embedded DoD-PKI certificates

  - CACs are issued at Real-time Automated Personnel Identification System (RAPIDS) terminals.
    - To locate a RAPIDS terminal near you, use http://www.dmdc.osd.mil/rsl/ to search by city, state, or zip code.
- Software certificates are issued by Local Registration Authorities (LRAs)
  - NOTE: Software-based certificates are discouraged because the certificates are stored as vulnerable files on a computer that the user may not have 100% control over.
  - These are used as a last resort when a CAC reader and middleware not available
- CAC users with government-furnished laptops must request a laptop CAC reader and middleware for the laptop.

Using the DoD-PKI Certificate on a CAC

- A CAC (smart–card) reader and software must be installed on the workstation
  - Installation of smart card readers and middleware is the responsibility of the command/agency that controls the workstation configuration. See below for contact information.
- Some applications, including Microsoft Outlook and Microsoft Internet Explorer, require configuration to install the certificates from a smart card into the application.
  - The private keys never leave the CAC card
  - The configuration step alerts the application that a certificate's private keys reside on the CAC.
  - This configuration is also the responsibility of the command that controls the workstation, but requires the CAC be present in the card reader to perform the configuration.
- The CAC must be inserted in the smart-card reader prior to use
- The CAC must be "unlocked" prior to use by entering the owner's CAC PIN when requested.
  - If the PIN is entered incorrectly four times in a row, the CAC will lock itself out and require a visit to a RAPIDS terminal or a CAC PIN Reset (CPR) station for unlocking
  - Contact the user's service/agency help desk to locate the nearest CPR.

Who Can Obtain a DoD-PKI Certificate?

- Eligible DoD-users are:
  - Active duty, uniformed services personnel
  - Reserve members,
  - DoD civilian employees
  - Personnel working on-site at DoD facilities using DoD network and e-mail services.
- Non-DoD military or civilian employees

  - Eligibility is determined based on the interaction of the individual with the DoD rather than on the type of individual.
    - DoD support-contractors
    - non-US nationals

How Do Contractors Obtain a DoD PKI Certificate?

- Must obtain certificates from DoD-approved external PKIs.
- http://iase.disa.mil/pki/eca

DoD PKI Certificate Frequently Asked Questions

- http://iase.disa.mil/pki

DoD PKI Help Desk operates around-the-clock (24x7)

- Services for PKI users at all levels
- Will take calls or e-mails from any DoD User/RA/LRA experiencing a problem with PKI
- disa-esmost@okc.disa.mil
- 1-800-490-1643, Option 5

IMPORTANT POCs from the DoD PKI Help Desk

Location	**Contact Numbers**	**Situation**
Army	1-866-738-3222	Army Set & ID Helpdesk - User Support for Army Personnel
	pki_reg@netcom.army.mil	Server Certificate Issues
	https://www.conus-tnosc.army.mil/	
	April.Bowman@us.army.mil	CAC Issues
	Nicole.Baker@us.army.mil	
	https://informationassurance.us.army.mil/cacpki/	UserName/Password REQUIRED Army Personnel
PKE Helpdesk	PKE_Support@disa.mil	Difficulty **downloading Server Certificates** or
	https://gesportal.dod.mil/sites/dodpke	having difficulty with **email ID Certificate** (use the email)
Contractor PKI certs	http://iase.disa.mil/pki/eca/index.html	Site for PKI info for contractors requesting PKI certs. Tells them how to go about getting them.
Navy	https://infosec.navy.mil/PKI/	Navy users. especially when they are looking for specific server information.
	https://warlord.spawar.navy.mil/PKI/index.html	Navy Personnel
DMDC	1-800-372-7437	Users having difficulties with **Certificates on Common Access Card (CAC)**
Deers/Rapids (aka DRAC)		

IASE	http://iase.disa.mil/	The PKI Bible page. All the important docs are here (RA/LRA/END USER manuals etc.)
PKI PMO Links	http://www.defenselink.mil/nii/org/sio/ia/pki/sites.html	It is handy if you need to find PKI info specific to a certain branch as it contains links to each branch's PKI website. Often, you can use these sites to track down LRAs or at least find branch-specific helpdesk numbers (i.e. Army's Set-D or Navy's Infosec) if you can't find the info yourself.
PKE Support Web	PKE_Support@disa.mil	PKE Support. -
		Server Cert Issues
	https://gesportal.dod.mil/sites/dodpke	Email Cert Issues
Check for certs on PKI	https://ds-web.c3pki.chamb.disa.mil/	A quick way to search and verify you have a certificate. If the user is NOT in the database, then their LRA or RA will have to reissue a certificate. Sometimes the certificate will appear to have been downloaded, but if there was any problem downloading, then the UDF will have to be uploaded again because the download is only good for one shot. An end users RA/LRA can search this listing as well as search their "Certificate Block" for the end user. If the end user is not there, the end user has no certificate and the LRA will have to create a new one.
DOD411	https://dod411.chamb.disa.mil	
PKI Home Page	http://dodpki.c3pki.chamb.disa.mil/	
	http://dodpki.c3pki.den.disa.mil/	
PKI Identity Directory	https://ds-web.c3pki.chamb.disa.mil/id	
	https://ds-web.c3pki.den.disa.mil/id	
PKI Email Directory	https://ds-web.c3pki.chamb.disa.mil/mail	
	https://ds-web.c3pki.den.disa.mil/mail	
Software cert Registration	http://reg.c3pki.chamb.disa.mil/	
	http://reg.c3pki.den.disa.mil/	
Army-Europe PKI	https://iassure.usareur.army.mil/pki/	
AirForceDEERS/RAPIDS CAC	https://www.afpc.randolph.af.mil/deers/	
Marines	https://www.noc.usmc.mil/PKI/	
NGA	chdesk@nga.mil	1-800-455-0899

Steps to follow in case of questions/concerns/issues

- Users should contact their Service/Agency’s prescribed POC above if the user:
    - Cannot obtain a Common Access Card or DoD-PKI certificate
    - Can not view DoD-PKI certificate in their web browser
    - Is experiencing issues with the CAC, CAC reader, or CAC middleware
    - Is redirected to a page stating “user certificate is required”
    - Has problems with the web browser not seeing the DoD-PKI certificate
- Users should contact DISA’s DoD-PKI Help Desk as prescribed above if the user:
    - Is unable to get or see results from their own Service/Agency’s prescribed POC.
- Users should contact extranet@nga.mil if the user:
    - Is not able to get to https://www.extranet.nga.mil
    - Has not received approval to access the NGA PKE-NIPRNet
    - Has questions/concerns/issues about filling out registration